Über die vollständige Auflösung der algebraischen Gleichungen im Bereiche einer rationalen Primzahl mit Hülfe des Newton'schen Diagrammes.

Inaugural-Dissertation

zur

Erlangung der Doktorwürde

der

Hohen philosophischen Fakultät der Universität Marburg

vorgelegt von

PHILIPP VOLL

aus Frankfurt a. M.

Marburg 1915.

Druck von C. Naumann's Druckerei in Frankfurt a. M.

Über die vollständige Auflösung der algebraischen Gleichungen im Bereiche einer rationalen Primzahl mit Hülfe des Newton'schen Diagrammes.

Inaugural-Dissertation

zur

Erlangung der Doktorwürde

der

Hohen philosophischen Fakultät der Universität Marburg

ACAD.
LUGD.BAT.
BIBL.

vorgelegt von

PHILIPP VOLL
aus Frankfurt a. M.

Marburg 1915.

Druck von C. Naumann's Druckerei in Frankfurt a. M.

Von der Fakultät als Dissertation angenommen am 2. März 1915.

Berichterstatter: Geh. Reg.-Rat Prof. Dr. Hensel.

Literaturnachweis.

Hensel, Theorie der algebraischen Zahlen. Leipzig und Berlin 1908.
(In der Abhandlung durch H bezeichnet.)

Hensel und Landsberg, Theorie der algebraischen Funktionen einer Variablen. Leipzig 1902.
(In der Abhandlung durch H und L bezeichnet.)

Weber, Lehrbuch der Algebra II. Braunschweig 1899.

Dumas, „Sur quelques cas d'irréductibilité des polynomes à coefficients rationnels" in Journal de Mathématiques pures et appliquées, 6. Serie, Band II. 1906.

Digitized by the Internet Archive
in 2026

https://archive.org/details/IA41556035_0093

In dem Werke: Hensel und Landsberg, „Theorie der algebraischen Funktionen einer Variabeln“ führt Herr Geheimrat Hensel die Aufgabe durch, die n Wurzeln der Gleichung

$$f(u, z) = A_0(z) + A_1(z)\, u + A_2(z)\, u^2 + \cdots + A_n(z)\, u^n = 0$$

mit beliebigen rationalen Funktionen von z als Koeffizienten in endlicher Umgebung einer beliebigen Stelle $(z = \alpha)$ durch konvergente Reihen

$$u = v_0 (z-\alpha)^{h_0} + v_1 (z-\alpha)^{h_1} + \cdots$$

darzustellen, die nach steigenden Potenzen des zugehörigen Linearfaktors fortschreiten (H & L S. 40 ff.).

In der Vorrede zur „Theorie der algebraischen Zahlen“ weist Herr Geheimrat Hensel auf die fruchtbringende Übertragung der Methoden der Funktionentheorie in das Gebiet der algebraischen Zahlen hin (H S. IV ff.). Es wird dort besonders hervorgehoben, daß, wie in der Theorie der algebraischen Funktionen, jedem Werte $z=\alpha$ der willkürlichen Veränderlichen eine Anzahl von Punkten der zugeordneten Riemannschen Fläche entspricht, in der Theorie der algebraischen Zahlen jeder reellen Primzahl p eine bestimmte Anzahl von Stellen zugeordnet ist, und daß alle algebraischen Zahlen eines Körpers $K(\gamma)$ sich für den Bereich einer solchen Stelle in Reihen entwickeln lassen, die nach ganzen Potenzen einer algebraischen Entwicklungszahl fortschreiten und algebraische Koeffizienten haben.

In dem angezogenen Werke wird ferner gezeigt, daß, wenn e die Ordnung und f der Grad der betreffenden Entwicklungszahl ist, als Koeffizienten der eben erwähnten Potenzreihen stets $(p^f-1)^{\text{te}}$ Einheitswurzeln gewählt werden können, während alsdann die Entwicklungszahl π als Wurzel einer Eisensteinschen Gleichung

$$\Psi(x, \eta) = x^e + p\, c_{e-1}\, x^{e-1} + \cdots + p\, c_0 = 0$$

genommen werden kann, deren Koeffizienten c_i ganze Zahlen desjenigen Körpers sind, der durch die Entwicklungskoeffizienten der Potenzreihe, also durch die $(p^f-1)^{\text{ten}}$ Einheitswurzeln, konstituiert wird. (H S. 180 ff.)

Es liegt nun nahe, die bei der zu Anfang genannten Aufgabe aus der Funktionentheorie (H & L S. 40 ff.) gebrauchte Methode in das

Gebiet der algebraischen Zahlen zu übertragen bei der Lösung folgender Frage:

Gegeben ist eine Gleichung

$$f(u, p) = A_0(p) + A_1(p)\, u + A_2(p)\, u^2 + \cdots + A_n(p)\, u^n = 0 \quad (p)$$

mit rationalen p-adischen Zahlen $A_i(p)$ als Koeffizienten. Die Wurzeln dieser Gleichung für den Bereich von p sind algebraische p-adische Zahlen. Es sollen diese Wurzeln durch Potenzreihen dargestellt werden, die von der eben charakterisierten Art sind, d. h. es soll insbesondere die Eisensteinsche Gleichung bestimmt werden, der die Entwicklungszahl dieser Potenzreihen genügt, und gezeigt werden, wie die Entwicklungskoeffizienten der Potenzreihen als Einheitswurzeln zu ermitteln sind.

Wir überzeugen uns zunächst von der Möglichkeit der Übertragung der in H & L S. 40 ff. dargelegten Methode auf unsere Aufgabe.

Die rationalen p-adischen Zahlen $A_i(p)$, die als Koeffizienten der obigen Gleichung

$$f(u, p) = 0 \qquad (p)$$

auftreten, lassen sich bekanntlich allgemein in Reihen

$$A_i(p) = a_i\, p^{\varrho_i} + b_i\, p^{\varrho_i + 1} + c_i\, p^{\varrho_i + 2} + \cdots$$

entwickeln, die nach ganzen Potenzen der Primzahl p fortschreiten, und in denen die Größen a_i Zahlen der Reihe

$$1, 2, \cdots\cdots, (p-1),$$

die b_i, c_i u. s. w. Zahlen der Reihe

$$0, 1, 2, \cdots\cdots, (p-1)$$

sind. Setzen wir nun u_o, eine Wurzel unserer Gleichung, in der Form

$$u_o = \eta_o \pi^{q_0} + \eta_1 \pi^{q_0 + 1} + \eta_2 \pi^{q_0 + 2} + \cdots$$

an, wo η_i die noch zu bestimmenden $(p^f - 1)^{\text{ten}}$ Einheitswurzeln, nämlich die Entwicklungskoeffizienten der Reihe bedeuten, und π die noch zu ermittelnde Entwicklungszahl darstellt, so ist ja im allgemeinsten Falle

$$\pi = p^{\frac{1}{e}} \varepsilon,$$

wo ε eine algebraische Einheit *modulo* p ist (H S. 148). — Es ist also

$$u_0 = \eta_0 \varepsilon^{q_0} \cdot p^{\frac{q_0}{e}} + \eta_1 \varepsilon^{q_0+1} p^{\frac{q_0+1}{e}} + \eta_2 \varepsilon^{q_0+2} \cdot p^{\frac{q_0+2}{e}} + \cdots$$

Hierin ist jedes Produkt

$$\eta_i \cdot \varepsilon^{q_0+i}$$

eine algebraische Einheit *modulo* p, da dies sowohl für die η_i als auch die ganzzahligen Potenzen ε^{q_0+i} von ε gilt, und das Produkt zweier solchen Einheiten wieder eine solche Einheit ist.

Setzen wir

$$\eta_i \cdot \varepsilon^{q_0+i} = \varepsilon_i$$

und

$$\frac{q_0+i}{e} = t_i ,$$

so haben wir in

$$u_0 = \varepsilon_0 p^{t_0} + \varepsilon_1 p^{t_1} + \varepsilon_2 p^{t_2} + \cdots$$

eine nach ganzen Potenzen von $p^{\frac{1}{e}}$ fortschreitende Potenzreihe, deren Koeffizienten ε_i algebraische Einheiten *modulo* $p^{\frac{1}{e}}$ sind, da sie dies *modulo* p sind.

Substituieren wir sowohl die Reihen für die Gleichungskoeffizienten $A_i(p)$ als auch diese Reihe für u_0 in der Gleichung $f(u, p) = 0$, so geht deren linke Seite, wenn man sie nach gleich hohen Potenzen von $p^{\frac{1}{e}}$ ordnet, in eine nach ganzen Potenzen von $p^{\frac{1}{e}}$ fortschreitende Reihe über

$$f(u_0, p) = C_0 p^{g_0} + C_1 p^{g_1} + \cdots$$

Nun ist u_0 nur dann eine Wurzel der Gleichung $f(u, p) = 0$ für den Bereich von p, wenn die Näherungswerte genügend hoher Ordnung von $f(u_0, p)$ durch jede noch so hohe Potenz von p algebraisch teilbar sind.

Daraus ergibt sich die Forderung, u_0 so zu bestimmen, daß zunächst

$$C_0 \equiv 0 \ (mod\ p^{\frac{1}{e}})$$

wird.

Durch Einsetzen der Reihenentwickelungen für die Koeffizienten $A_i(p)$ und der Reihe für u_0 in die gegebene Gleichung $f(u, p) = 0$ erhält man auf deren linker Seite

$$\left.\begin{aligned} f(u_0, p) = &\left(a_0 p^{\varrho_0} + b_0 p^{\varrho_0+1} + \cdots\right) \\ &+ \left(a_1 p^{\varrho_1} + \cdots\right)\left(\varepsilon_0 p^{t_0} + \varepsilon_1 p^{t_1} + \cdots\right) \\ &+ \left(a_2 p^{\varrho_2} + \cdots\right)\left(\varepsilon_0 p^{t_0} + \cdots\right)^2 + \cdots + \left(a_n p^{\varrho_n} + \cdots\right)\left(\varepsilon_0 p^{t_0} + \cdots\right)^n \end{aligned}\right\}$$

Die Summe der Anfangsglieder der $(n+1)$ Posten auf der rechten Seite dieser Gleichung ist

$$f_0(p) = a_0 p^{\varrho_0} + a_1 \varepsilon_0 p^{\varrho_1 + t_0} + a_2 \varepsilon_0^{\,2} p^{\varrho_2 + 2t_0} + \cdots + a_n \varepsilon_0^{\,n} p^{\varrho_n + nt_0}$$

Bildet man die Summe aller derjenigen Posten von $f_0(p)$, deren Exponenten $\varrho_i + it_0$ den kleinsten Wert haben (t_0 dabei als gegeben betrachtet), so ergibt sich darin das Anfangsglied $C_0 p^{g_0}$ von $f(u_0, p)$.

Ganz entsprechend wie in der Betrachtung H & L S. 42 darf auch hier t_0 nur so bestimmt werden, daß mindestens zwei der Exponenten auf der rechten Seite von $f_0(p)$ einander gleich sind und den kleinsten Wert unter den $\varrho_i + it_0$ haben. Denn wäre nur eines der $\varrho_i + it_0$ vom kleinsten Werte, etwa $\varrho_k + kt_0$, so hieße das Anfangsglied der Entwicklung von $f(u_0, p)$

$$a_k \varepsilon_0^{\,k} p^{\varrho_k + kt_0}.$$

u_0 könnte nur dann eine Wurzel der Gleichung $f(u, p) = 0$ für den Bereich von p sein, wenn

$$\varepsilon_0^{\,k} \equiv 0 \left(mod\ p^{\frac{1}{e}}\right)$$

wäre, da

$$a_k \not\equiv 0 \left(mod\ p^{\frac{1}{e}}\right)$$

ist. Daraus ergäbe sich aber die Forderung, daß die ganzzahlige Potenz $\varepsilon_0{}^k$ einer algebraischen Einheit ε_0 *modulo* $p^{\frac{1}{e}}$ durch $p^{\frac{1}{e}}$ teilbar wäre, was mit eben diesem Charakter von ε_0 unvereinbar ist.

Man sieht schon aus diesen wenigen Darlegungen, daß die Übertragung der fraglichen Methode in unser Problem bis jetzt eine fast wörtliche ist, nur treten an Stelle von Gleichungen zur Ermittlung der ε_i in der Funktionentheorie hier in der Zahlentheorie Kongruenzen.

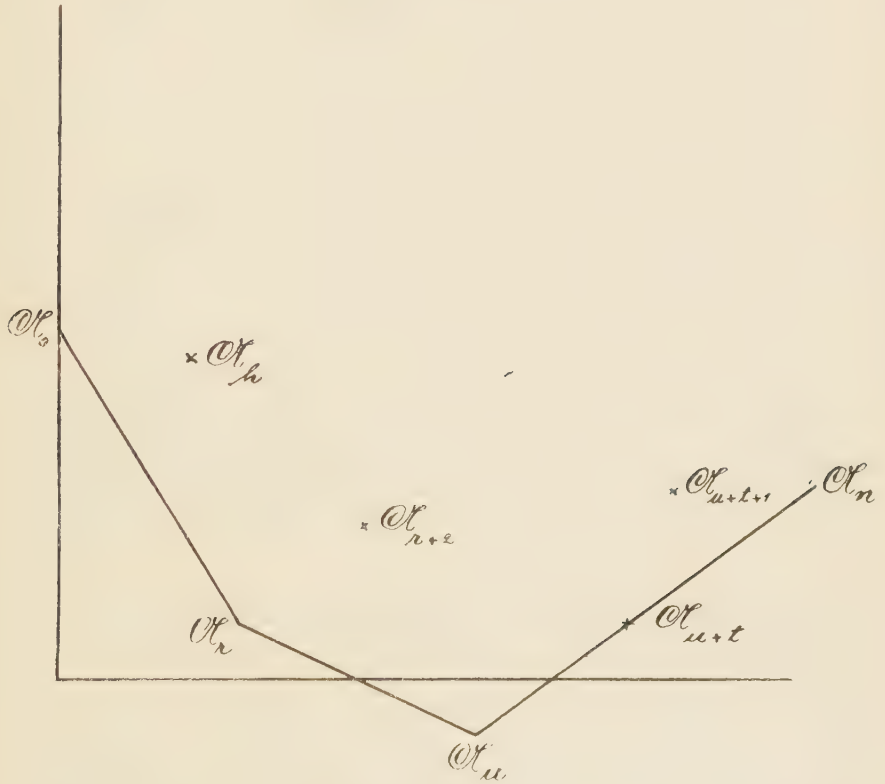
Insbesondere überzeugt man sich sofort aus H & S S. 43 Zeile 4 ff., daß der Exponent t_0 des Anfangsgliedes von u_0 genau in der gleichen Weise wie dort bestimmt werden kann, weshalb auf die Darlegung hier verzichtet werden kann. Der einzige Unterschied ist der, daß wir unter den ϱ_i nicht die Ordnungszahl von $A_i(z)$ in Bezug auf die zu untersuchende Stelle ($z = \alpha$) verstehen, sondern die Ordnungszahl der ratio-

nalen p-adischen Zahl $A_i(p)$ in Bezug auf p. Es genügt, hier das Ergebnis anzuführen:

In einem rechtwinkligen Koordinatensystem lege man die Punkte

$$\mathfrak{A}_0 = (0, \varrho_0),\ \mathfrak{A}_1 = (1, \varrho_1),\ \mathfrak{A}_2 = (2, \varrho_2),$$

fest. $$\ldots\ \mathfrak{A}_n = (n, \varrho_n)$$



$\mathfrak{A}_n$ verbindet man mit demjenigen Punkte $\mathfrak{A}_u$, der, von $\mathfrak{A}_n$ aus gesehen, am tiefsten liegt. Liegen mehrere Punkte auf der Richtung $\mathfrak{A}_n\ \mathfrak{A}_u$, so ist $\mathfrak{A}_u$ als äußerster zu wählen (vergl. Figur). $\mathfrak{A}_u$ wird dann wieder mit demjenigen Punkte $\mathfrak{A}_r$ verbunden, dessen Index r kleiner als u ist, und der von $\mathfrak{A}_u$ aus betrachtet am tiefsten und äußersten liegt, u. s. w., bis schließlich das nach unten konvexe Begrenzungspolygon $\mathfrak{A}_n\ \mathfrak{A}_u\ \mathfrak{A}_r\ \ldots\ \mathfrak{A}_0$ entsteht. Alsdann ist endlich t_0 so zu wählen, daß es der Steigung einer der Begrenzungssehnen gleich ist.

Weiter ergibt sich analog H & L S. 44 Zeile 2 v. u. u. ff., daß der Koeffizient C_0 des Anfangsgliedes $C_0\, p^{g_0}$ in der Entwicklung von $f(u_0, p)$

aus der Summe aller und nur der Produkte $a_r \varepsilon_0{}^r$ besteht, für die die zugeordneten Punkte $\mathfrak{A}_r$ auf der gewählten Begrenzungssehne mit der Steigung t_0 liegen. Sind dies gerade die Punkte $\mathfrak{A}_l$, $\mathfrak{A}_k$, $\mathfrak{A}_i$, ... $\mathfrak{A}_h$, $\mathfrak{A}_g$, so heißt also der Koeffizient C_0:

$$\left.\begin{aligned}\varphi(\varepsilon_0) = a_l \cdot \varepsilon_0{}^l + a_k \cdot \varepsilon_0{}^k + a_i \varepsilon_0{}^i + \cdots \\ + a_h \varepsilon_0{}^h + a_g \cdot \varepsilon_0{}^g .\end{aligned}\right\}$$

Nun war bekanntlich u_0 so zu bestimmen, daß

$$C_0 \equiv 0 \left(mod\ p^{\frac{1}{e}}\right)$$

ist. Es ergibt sich also jetzt die Forderung, ε_0 als Kongruenzwurzel der Kongruenz

$$\varphi_0(\varepsilon) \equiv 0 \left(mod\ p^{\frac{1}{e}}\right)$$

zu wählen, wobei von etwaigen Lösungen

$$\varepsilon_0 \equiv 0 \left(mod\ p^{\frac{1}{e}}\right)$$

abzusehen ist, da ja ε_0 algebraische Einheit *modulo* $p^{\frac{1}{e}}$ sein soll.

Daß und wie dieser Forderung genügt werden kann, werden wir später eingehend zeigen. Es sei daher im folgenden vorausgesetzt.

Die Darstellung des Anfangsglieds $\varepsilon_0 p^{t_0}$ ist hiermit im Prinzip geschildert.

Da es uns nur auf die Entwicklung einer Wurzelreihe und die Darstellung von deren Entwickelungszahl und Koeffizienten ankommt, wollen wir konform mit der Behandlung in H & L S. 50 ff. t_0 als Steigung der letzten Begrenzungssehne $\mathfrak{A}_r\,\mathfrak{A}_0$ wählen, dann ist t_0 die maximale Steigung, die im zugehörigen Begrenzungspolygon auftritt. Wörtlich kann alsdann wieder die Darstellung des 2. Entwickelungsglieds $\varepsilon_1 p^{t_1}$ und der folgenden aus H & L S. 50 ff. übernommen werden, wenn wir nur statt ζ die Größe p setzen und bedenken, daß für die Bestimmung der ε_1, ε_2, u. s. w. nicht Gleichungen, sondern Kongruenzen *modulo* $p^{\frac{1}{e}}$ in Frage kommen. Kurz, wir bilden die Gleichung n. Grads

$$\left.\begin{aligned}f\left(\varepsilon_0 p^{t_0} + u'\right) = f\left(\varepsilon_0 p^{t_0}\right) + u' \frac{f'\left(\varepsilon_0 p^{t_0}\right)}{1} \\ + u'^2 \frac{f''\left(\varepsilon_0 p^{t_0}\right)}{1 \cdot 2} + \cdots + u'^n \frac{f^{(n)}\left(\varepsilon_0 p^{t_0}\right)}{1 \cdot 2 \cdots n},\end{aligned}\right\}$$

wobei unter u' die gesuchte Wurzelreihe u_0 mit Ausschluß ihres ersten Gliedes $\varepsilon_0 p^{t_0}$ zu verstehen ist. Bezeichnen wir den Koeffizienten von u'^k nämlich

$$\frac{f^{(k)}\left(\varepsilon_0 p^{t_0}\right)}{1 \cdot 2 \cdot \cdots \cdot k},$$

allgemein mit $A'_k(p)$, so ist die Gleichung n. Grades

$$f\left(\varepsilon_0 p^{t_0} + u'\right) = A'_0(p) + A'_1(p)\, u' + A'_2(p)\, u'^2 + \cdots + A'_n(p)\, u'^n$$

genau wie die Gleichung $f(u, p) = 0$ zu behandeln, d. h. die Koeffizienten $A'_k(p)$ werden nach Potenzen von $p^{\frac{1}{e}}$ entwickelt, was möglich ist, da der reduzierte Nenner von t_0 entweder e oder ein Teiler von e ist.

Dann wird mit Hilfe der Ordnungszahlen ϱ'_k der Koeffizienten $A'_k(p)$ in Bezug auf p ein zweites Diagramm aus den Punkten $\mathfrak{A}'_k$ beziehlich mit Koordinaten (k, ϱ'_k) konstruiert. Man bildet genau wie im ersten Falle für dieses 2. Diagramm das nach unten konvexe Begrenzungspolygon und setzt t_1 gleich der maximalen Steigung, die unter den Begrenzungssehnen auftritt. Daß wir auch hier wieder die maximale Steigung wählen, wird sich aus der späteren Betrachtung rechtfertigen.

Der Koeffizient ε_1 des zweiten Glieds $\varepsilon_1 p^{t_1}$ unserer Wurzelreihe u_0 ist als Kongruenzwurzel der Kongruenz

$$\varphi_1(\varepsilon) \equiv 0 \left(mod\ p^{\frac{1}{e}}\right)$$

zu wählen, wobei, wenn die Entwickelung der $A'_k(p)$ nach Potenzen von p allgemein mit dem Gliede

$$a'_k p^{\varrho'_k}$$

beginnt, unter $\varphi_1(\varepsilon)$ die Summe

$$a'_s \varepsilon^s + \cdots + a'_i \varepsilon^i + a'_0$$

von denjenigen Posten $a'_i \varepsilon^i$ zu verstehen ist, für die die zugeordneten Punkte $\mathfrak{A}'_i$ wieder gerade auf der Begrenzungssehne maximaler Steigung des 2. Diagramms liegen.

Wir werden später bei der Behandlung der Kongruenzwurzeln von

$$\Phi_0(\varepsilon) \equiv 0 \left(mod\ p^{\frac{1}{e}}\right)$$

auch über die Kongruenzwurzeln von

$$\Phi_1(\varepsilon) \equiv 0 \left(mod\ p^{\frac{1}{e}}\right)$$

näheren Aufschluß bringen.

Durch fortgesetzte Anwendung dieses Verfahrens lassen sich die Glieder der Wurzelreihe

$$u_0 = \varepsilon_0 p^{t_0} + \varepsilon_1 p^{t_1} + \varepsilon_2 p^{t_2} + \cdots$$

soweit man will berechnen. (Vergl. H & L S. 52 Mitte.)

Daß u_0 in der Tat eine Wurzel der Gleichung $f(u, p) = 0$ für den Bereich von p ist, wenn die Glieder von u_0 genügend weit berechnet sind, erkennt man daraus, daß offenbar die Ordnungszahlen in Bezug auf p in der Reihe der Ausdrücke

$$f(u, p),\ f\left(\varepsilon_0 p^{t_0} + u'\right),\ f\left(\varepsilon_0 p^{t_0} + \varepsilon_1 p^{t_1} + u''\right),$$
$$f\left(\varepsilon_0 p^{t_0} + \varepsilon_1 p^{t_1} + \varepsilon_2 p^{t_2} + u'''\right) \cdots$$

stets wachsen, je weiter man in dieser Reihe fortschreitet.

Damit ist die Übertragbarkeit der fraglichen Methode aus der Funktionentheorie auf unser zahlentheoretisches Problem gezeigt.

Wir unterziehen nun das im Großen charakterisierte Verfahren einer genaueren Untersuchung. Dabei setzen wir jedoch voraus, daß die Primzahl p größer ist als der Grad der gegebenen Gleichung. Wäre nämlich p nicht größer als der Grad der Gleichung, so wäre es, da das Produkt $e.f$ aus der Ordnung e des Primteilers π und seinem Grad f kleiner als der Grad der Gleichung oder gleich demselben ist, nicht ausgeschlossen, daß

$$e \equiv 0\ (mod\ p)$$

wäre, und für diesen Fall würden die folgenden Ableitungen nicht gelten. (Vgl. H S. 201 Mitte.)

Gegeben sei jetzt eine im Bereich der rationalen p-adischen Zahlen irreduzible Gleichung λ^{ten} Grades mit rationalen p-adischen Zahlen als Koeffizienten:

$$f(u) = 0 \qquad (p)$$

Es soll das fragliche Verfahren für diese Gleichung untersucht werden.

Dann besitzt das oben erwähnte Diagramm der Funktion $f(u)$ nach *Dumas „Sur quelques cas d' irréductibilité des polynomes à coefficients rationnels"* eine einzige Begrenzungssehne s_m. Diese besitzt, wenn e die Ordnung des gesuchten Primteilers ist, sicher eine Steigung $\frac{m}{e}$, wo m eine positive oder negative ganze Zahl oder Null ist. Denn $p^{\frac{m}{e}}$ gibt ja, wie wir sahen, den absoluten Betrag des 1. Entwickelungsglieds unserer Wurzelreihe u_o für den Bereich von p an, und da diese, wenn e die Ordnung von π ist, nach Potenzen von $p^{\frac{1}{e}}$ fortschreitet, so muß sich die Steigung von s_m in der Form $\frac{m}{e}$ darstellen lassen; die reduzierte Form von $\frac{m}{e}$ möge $\frac{m_1}{e_1}$ heißen.

Unter der Voraussetzung

$$p > \lambda ,$$

die, wie wir eben zeigten, die Voraussetzung

$$e \not\equiv 0 \ (mod\ p)$$

in sich schließt, kann nun der Primteiler π so gewählt werden, daß er der Gleichung

$$\pi^{e} = \eta^{k_0} \cdot p$$

genügt, worin η eine primitive $(p^f - 1)^{te}$ Einheitswurzel und k_0 eine der Zahlen

$$0,\ 1,\ 2,\ \ldots,\ (e_0 - 1)$$

ist, wenn $e_0 = (e,\ p^f - 1)$ ist.

(Vgl. H S. 203).

Diese Gleichung wird später eindeutig bestimmt werden. Jetzt wollen wir aus ihr nur Schlüsse über die Beschaffenheit der Kongruenzen

$$\varphi_i(\varepsilon) \equiv 0 \ \left(mod\ p^{\frac{1}{e}}\right),$$

wie wir oben ankündigten, ziehen. Es sind diese jene Kongruenzen, die uns, wenn wir u_0 in der Form schreiben (vergl. S. 7)

$$u_0 = \varepsilon_0\, p^{t_0} + \varepsilon_1\, p^{t_1} + \varepsilon_2\, p^{t_2} + \ldots ,$$

die Koeffizienten ε_i nach den obigen Betrachtungen liefern sollen.

Setzt man nämlich $\pi = p^{\frac{1}{e}} \varepsilon$ (vgl. S. 6) und dividiert, nachdem man für π eingesetzt hat, die Gleichung

$$\pi^e = \eta^{k_0} p$$

durch p, so genügt die algebraische Einheit ε *modulo* p der erhaltenen Gleichung

$$\varepsilon^e = \eta^{k_0} \qquad (p) \ .$$

Die Wurzeln dieser Gleichung mögen

$$\varepsilon_1^{(0)}, \ \varepsilon_2^{(0)}, \ \ldots \ , \ \varepsilon_e^{(0)}$$

sein, endlich seien die Wurzeln derjenigen Gleichung, deren rechte Seite aus der letzten Gleichung dadurch hervorgeht, daß η durch η^{p^k} ersetzt wird, der Reihe nach $\varepsilon_1^{(k)}, \ \varepsilon_2^{(k)}, \ \ldots \ \varepsilon_e^{(k)}$.

Nimmt man nun noch an, daß das 1. Glied unserer Wurzelreihe u_0 als Entwickelungskoeffizienten die $(p^f-1)^{\text{te}}$ Einheitswurzel η_m besitzt, und berücksichtigt die Darlegungen in H S. 209 bis 213, so muß die Kongruenz

$$\Phi_m(\varepsilon) \equiv 0 \qquad \left(mod\ p^{\frac{1}{e}}\right),$$

die der Sehne s_m zugeordnet ist, folgende $\lambda = e \cdot f$ Kongruenzwurzeln besitzen:

$$\left.\begin{array}{l}
\eta_m \varepsilon_1^{(0)^m}, \ \eta_m \varepsilon_2^{(0)^m}, \ \ldots\ldots\ldots\ldots\ldots \ \eta_m \varepsilon_e^{(0)^m} \\
\quad - \ - \ - \ - \ - \ - \ - \ - \\
\eta_m^{p^k} \varepsilon_1^{(k)^m}, \ \eta_m^{p^k} \varepsilon_2^{(k)^m}, \ \ldots\ldots\ldots\ldots\ldots \ \eta_m^{p^k} \varepsilon_e^{(k)^m} \\
\quad - \ - \ - \ - \ - \ - \ - \ - \\
\eta_m^{p^{f-1}} \varepsilon_1^{((f-1))^m}, \ \eta_m^{p^{f-1}} \varepsilon_2^{((f-1))^m}, \ \ldots \ \eta_m^{p^{f-1}} \varepsilon_e^{((f-1))^m}
\end{array}\right\} \begin{array}{l} f \\ \text{Zeilen} \end{array}$$

e Spalten $\qquad (e \cdot f = \lambda).$

(NB! Die Bezeichnungen lehnen sich möglichst an die Darlegungen in H S. 209—213 an.)

Ist $x^e = a$, so genügen die x_1^m, x_2^m, $\cdots$ x_e^m, wenn x_1, $x_2 = x_1\,\omega_e$, $x_3 = x_1\,\omega_e^2$, $\cdots$ $x_e = x_1\,\omega_e^{e-1}$

[wobei ω_e eine primitive $(e)^{\text{te}}$ Einheitswurzel bedeutet] die Wurzeln von $x^e = a$ sind, der Gleichung

$$\left[(x^m)^{e_1} - a^{m_1}\right]^{(m,\,e)} = 0.$$

Hierbei ist $m = (m,e)\,.\,m_1$,
$e = (m,e)\,.\,e_1$.

Also genügen die $\varepsilon_1^{(0)^m}$, $\varepsilon_2^{(0)^m}$, $\cdots$ $\varepsilon_e^{(0)^m}$ der Gleichung

$$\left[\left(\varepsilon^{(0)^m}\right)^{e_1} - \eta^{k_0\,m_1}\right]^{(m,\,e)} = 0.$$

Oder, da die Koeffizienten und Wurzeln Einheiten *mod. p* sind, so genügen die $\varepsilon_1^{(0)^m}, \cdots \varepsilon_e^{(0)^m}$ der Kongruenz

$$\left[\left(\varepsilon^{(0)^m}\right)^{e_1} - \eta^{k_0\,m_1}\right]^{\frac{e}{e_1}} \equiv 0 \qquad (mod\ p),$$

wobei für $(m,\ e)$ das ihm gleiche $\frac{e}{e_1}$ gesetzt wurde. Daraus ergibt sich sofort, daß die

$$\eta_m\,\varepsilon_1^{(0)^m},\ \eta_m\,\varepsilon_2^{(0)^m},\ \cdots\ \eta_m\,\varepsilon_e^{(0)^m},$$

weil η_m Einheit *mod. p* ist, der Kongruenz genügen

$$\left[\left(\eta_m\,.\,\varepsilon^{(0)^m}\right)^{e_1} - \eta_m^{e_1}\,.\,\eta^{k_0\,m_1}\right]^{\frac{e}{e_1}} \equiv 0 \qquad (mod\ p)$$

Entsprechend genügen die $\eta_m^{p^k}\,.\,\varepsilon_1^{(k)^m}, \ldots\ \eta_m^{p^k}\,.\,\varepsilon_e^{(k)^m}$ der Kongruenz

$$\left[\left(\eta_m^{p^k}\,.\,\varepsilon^{(k)^m}\right)^{e_1} - \eta_m^{e_1\,.\,p^k}\,.\,\eta^{k_0\,m_1\,.\,p^k}\right]^{\frac{e}{e_1}} \equiv 0 \quad (mod\ p)$$

u. s. f.

Nun ist $\eta_m^{e_1}\,.\,\eta^{k_0\,m_1}$ sicher eine $(p^f - 1)^{\text{te}}$ Einheitswurzel, für die wir kurz η_σ setzen. Dann ergibt sich, daß

$$\varphi_m \equiv \left[\left(x^{e_1} - \eta_\sigma\right)\left(x^{e_1} - \eta_\sigma^{p}\right)\cdots\left(x^{e_1} - \eta_\sigma^{p^k}\right)\cdots\right.$$
$$\left.\left(x^{e_1} - \eta_\sigma^{p^{f-1}}\right)\right]^{\frac{n}{e_1}} \qquad (mod\ p).$$

Gesetzt, η_σ paßt zum Exponenten f_1, einem Teiler von f, so ist

$$\varphi_m \equiv \left[\left(x^{e_1} - \eta_\sigma\right)\left(x^{e_1} - \eta_\sigma^{p}\right) \cdots \left(x^{e_1} - \eta_\sigma^{p^{f_1-1}}\right)\right]^{\frac{e}{e_1}\cdot\frac{f}{f_1}} \quad (mod\ p)$$

und auch $\left(mod\ p^{\frac{1}{e}} \mathfrak{S}\ \mathfrak{p}\right)$.

In der eckigen Klammer steht, wenn $x^{e_1} = w$ gesetzt wird, eine auch *mod p* irreduzible Funktion $(f_1)^{\text{ten}}$ Grads in w, *mod p* betrachtet mit Zahlen der Reihe 0, 1 $\cdots$, $(p-1)$ als Koeffizienten.

Das 1. Glied einer der Wurzelreihen von $f(u) = 0$ ergibt sich also wie folgt:

Man setzt in dem mit Hilfe des 1. Diagramms ermittelten φ_m

$$x^{e_1} = w.$$

Dies ist möglich, ohne daß gebrochene Potenzen von w auftreten, da bei der Steigung $\frac{m_1}{e_1}$ der Mindest-Horizontalabstand zweier von der Sehne getroffener Diagrammpunkte gleich c_1 ist, also in φ_m nur Potenzen von x^{e_1} als Unbekannte vorkommen. Darauf zerlegt man die erhaltene Funktion in w *mod p* in ihre irreduzibelen Faktoren und bekommt dabei die $\left(\frac{e}{e_1}\cdot\frac{f}{f_1}\right)^{\text{te}}$ Potenz eines Primfaktors $(f_1)^{\text{ten}}$ Grads in w. Bezeichnet man eine Kongruenzwurzel *mod p* dieses Primfaktors mit w_1, was also eine $(p^{f_1} - 1)^{\text{te}}$ Einheitswurzel ist, so lautet das gesuchte Entwickelungsglied

$$w_1^{\frac{1}{e_1}} \cdot p^{\frac{m_1}{e_1}}.$$

Das 2. Entwickelungsglied derselben Wurzel von $f(u) = 0$ erhält man durch ganz entsprechende Behandlung der Gleichung λ. Grades

$$f\left(w_1^{\frac{1}{e_1}} \cdot p^{\frac{m_1}{e_1}} + u'\right) = 0.$$

Aus einer einfachen Überlegung ergibt sich nun, daß diese Gleichung uns genau soviel 2. Entwickelungsglieder liefert, als der Grad der Vielfachheit von $w_1^{\frac{1}{e_1}}$ unter den Kongruenzwurzeln von φ_m angibt. Man zeigt aber leicht, daß dieser Grad gleich

$$\frac{e}{e_1}\cdot\frac{f}{f_1} \quad \text{ist.}$$

Nämlich, die $e_1 . f_1$ Kongruenzwurzeln der eckigen Klammer von φ_m seien die folgenden:

$$\left.\begin{array}{lll}
\sqrt[e_1]{\eta_\sigma \cdot \omega_{e_1}^{1}} , & \sqrt[e_1]{\eta_\sigma^{p} \omega_{e_1}^{1}}, \ldots . & \sqrt[e_1]{\eta_\sigma^{p^{f_1-1}} \omega_{e_1}^{1}} \\
\sqrt[e_1]{\eta_\sigma \cdot \omega_{e_1}^{2}} , & \sqrt[e_1]{\eta_\sigma^{p} \omega_{e_1}^{2}}, \ldots . & \sqrt[e_1]{\eta_\sigma^{p^{f_1-1}} \omega_{e_1}^{2}} \\
\cdots\cdots\cdots & \cdots\cdots\cdots & \cdots\cdots\cdots \\
\sqrt[e_1]{\eta_\sigma \cdot \omega_{e_1}^{e_1}} , & \sqrt[e_1]{\eta_\sigma^{p} \omega_{e_1}^{e_1}}, \ldots . & \sqrt[e_1]{\eta_\sigma^{p^{f_1-1}} \omega_{e_1}^{e_1}}
\end{array}\right\} \begin{array}{l} e_1 \\ \text{Zeilen.} \end{array}$$

f_1 Spalten,

wobei ω_{e_1} eine primitive $(e_1)^{\text{te}}$ Einheitswurzel bedeutet.

Alle in einer Zeile stehenden Kongruenzwurzeln sind *mod* p voneinander verschieden; denn wäre z. B. für

$$k \neq \mu, \text{ wo } \left.\begin{matrix} k \\ \mu \end{matrix}\right\} < f_1 \text{ sind,}$$

$$\sqrt[e_1]{\eta_\sigma^{p^k} \omega_{e_1}^{\lambda}} \equiv \sqrt[e_1]{\eta_\sigma^{p^\mu} \cdot \omega_{e_1}^{\lambda}} \qquad (mod\ \mathfrak{p}) ,$$

so ergibt sich durch Division durch $\omega_{e_1}^{\lambda}$ und nachherige Erhebung in die $(e_1)^{\text{te}}$ Potenz

$$\eta_\sigma^{p^k} \equiv \eta_\sigma^{p^\mu} \qquad (mod\ \mathfrak{p})$$

Dies ist aber unmöglich, da die

$$\eta_\sigma , \eta_\sigma^{p} , \eta_\sigma^{p^2} , \ldots \eta_\sigma^{p^{f_1-1}}$$

alle inkongruent *modulo* p sind. Gesetzt, es wäre etwa $\sqrt[e_1]{\eta_\sigma}$ kon-

gruent *modulo* $\mathfrak{p}$ einer Kongruenzwurzel, die nicht mit ihm in derselben Zeile und Spalte steht, es wäre also etwa

$$\sqrt[e_1]{\eta_\sigma} \equiv \sqrt[e_1]{\eta_\sigma^{p^\mu}} \cdot \omega_{e_1}^{\nu} \pmod{\mathfrak{p}},$$

wo $\nu \not\equiv e_1$

$$\mu \begin{cases} \not\equiv 0 \\ < f_1 \end{cases}$$

so wäre auch

$$\sqrt[e_1]{\eta_\sigma}\ \omega_{e_1} \equiv \sqrt[e_1]{\eta_\sigma^{p^\mu}} \cdot \omega_{e_1}^{\nu+1} \pmod{\mathfrak{p}}$$

und $$\sqrt[e_1]{\eta_\sigma}\ \omega_{e_1}^2 \equiv \sqrt[e_1]{\eta_\sigma^{p^\mu}} \cdot \omega_{e_1}^{\nu+2} \pmod{\mathfrak{p}}$$

u. s. w.

Es wären also die Wurzeln von $x^{e_1} - \eta_\sigma \equiv 0 \pmod{\mathfrak{p}}$ den Wurzeln von

$$x^{e_1} - \eta_\sigma^{p^\mu} \equiv 0 \pmod{\mathfrak{p}}$$

beziehlich kongruent *modulo* $\mathfrak{p}$, d. h.
es wäre

$$x^{e_1} - \eta_\sigma \equiv x^{e_1} - \eta_\sigma^{p^\mu} \pmod{\mathfrak{p}}$$

oder

$$\eta_\sigma \equiv \eta_\sigma^{p^\mu} \pmod{\mathfrak{p}},$$

was falsch ist, da η_σ zum Exponenten f_1 paßt

und $\mu \begin{cases} \not\equiv 0 \\ < f_1 \end{cases}$, also η_σ und $\eta_\sigma^{p^\mu}$ inkongruent *modulo* $\mathfrak{p}$ sind.

Bleibt noch zu zeigen, daß alle in einer Spalte stehenden Kongruenzwurzeln zueinander inkongruent *modulo* p sind.

Gesetzt, es wäre

$$\sqrt[e_1]{\eta_\sigma \omega_{e_1}^{\bar{r}}} \equiv \sqrt[e_1]{\eta_\sigma \omega_{e_1}^{\bar{s}}} \pmod{\mathfrak{p}},$$

wo $\left.\begin{matrix}\bar{r}\\ \bar{s}\end{matrix}\right\} < e_1$ und $\bar{r} \neq \bar{s}$ seien,

dann wäre $\sqrt[e_1]{\eta_\sigma \omega_{e_1}^{\bar{s}}}\ (\omega_{e_1}^{\bar{r}-\bar{s}} - 1) \equiv 0 \pmod{\mathfrak{p}}$.

Nun ist $\sqrt[e_1]{\eta_\sigma \omega_{e_1}^{\bar{s}}} \not\equiv 0 \pmod{\mathfrak{p}}$,

denn die $(e_1)^{\text{te}}$ Potenz der linken Seite ist gleich η_σ, und dies ist Einheit *modulo* p; also müßte

$$\omega_{e_1}^{\bar{r}-\bar{s}} \equiv 1 \pmod{\mathfrak{p}} \text{ sein.}$$

Auf Grund dieser Kongruenz wäre $\omega_{e_1}^{\bar{r}-\bar{s}}$ Einheit unseres Bereichs. Nach dem Satze 3 auf S. 618 von Weber, Algebra II wäre $\omega_{e_1}^{\bar{r}-\bar{s}}$ dann und nur dann einer rationalen Zahl *modulo* p kongruent, wenn es der Kongruenz

$$x^{p-1} \equiv 1 \pmod{\mathfrak{p}}$$

genügt. Dieser Bedingung genügen aber unter den Einheitswurzeln, und eine solche ist ja $\omega_{e_1}^{\bar{r}-\bar{s}}$ nur die rationalen p=adischen Einheiten, und von diesen ist bekanntlich nur eine kongruent 1 *modulo* p, nämlich 1 selbst. Damit ist dargetan, daß, gegen die Voraussetzung, $\bar{r} - \bar{s} = 0$ sein müßte, und somit gezeigt, daß alle in einer Spalte stehenden Kongruenzwurzeln zueinander inkongruent sind.

Daher ist der Grad der Vielfachheit von $w_1^{\frac{1}{e_1}}$ unter den λ Kongruenzwurzeln von φ_m in der Tat $\frac{e}{e_1} \cdot \frac{f}{f_1}$.

Es soll jetzt die Anzahl der 2. Entwickelungsglieder bestimmt werden, die uns die Gleichung

$$f\left(w_1^{\frac{1}{e_1}} \cdot p^{\frac{m_1}{e_1}} + u'\right) = 0$$

liefert.

Nach H & L S. 54 können wir analog setzen

$$A'_k(p) = p^{\varrho_0 - k t_0} \frac{\varphi_m^{(k)}\left(\sqrt[e_1]{\eta_\sigma}\right)}{k!} + p^{\bar{\varrho}_0 - k t_0} \cdot \Phi_m^{(k)},$$

wo $p^{\bar{\varrho}_0}$ insbesondere der absolute Betrag von $A'_0(p)$ sein soll, und in dem 2. Posten alle übrigen Glieder von $A'_k(p)$ mit Ausnahme des Anfangsglieds zusammengefaßt sind.

Dann ist

$$\bar{\varrho}_0 > \varrho_0$$

Wenn $\frac{e}{e_1} \cdot \frac{f}{f_1}$ der Grad der Vielfachheit der Kongruenzwurzel $w_1^{\frac{1}{e_1}}$ der Kongruenz

$$\varphi_m(x) \equiv 0 \quad (\textit{modulo } \mathfrak{p}),$$

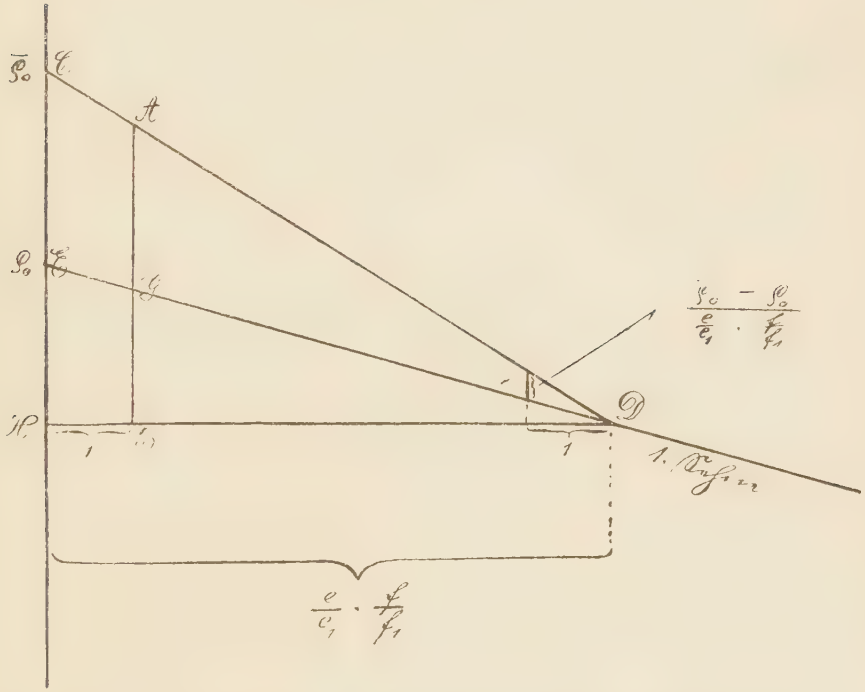
so ist

$$\frac{\varphi_m^{\left(\frac{e}{e_1} \cdot \frac{f}{f_1}\right)}\left(w_1^{\frac{1}{e_1}}\right)}{k!} \not\equiv 0 \quad (\textit{mod } \mathfrak{p}),$$

denn die durch das Differentiieren in dem Zähler auftretenden ganzzahligen Faktoren sind sicher kleiner als λ, und da $\lambda < p$, so kann durch sie die letzte Inkongruenz nicht gestört werden.

Der absolute Betrag von $A'_{\binom{c\,f}{e_1\,f_1}}(p)$ ist demnach

$$p^{\varrho_0 - \frac{c\,f}{e_1\,f_1}\,t_0}$$



d. h. aber, da t_0 die Steigung der Sehne des 1. Diagramms ist, nichts anderes als

$$\mathfrak{A}'_{\left(\frac{e\cdot f}{e_1\cdot f_1}\right)}$$

oder, wie es in der Figur heißt. D liegt auf eben dieser Sehne des 1. Diagramms.

Von den Punkten $\mathfrak{A}'_k$, für die $k < \frac{e\cdot f}{e_1\cdot f_1}$, zeigt man nun, daß sie entweder auf oder über der Sehne CD maximaler Steigung des 2. Diagramms liegen.

Wir zeigen dies jetzt für den Punkt $\mathfrak{A}_1'$. Es ist

$$A_0'(p) = p^{\varrho_0}\,\varphi_m\left(w_1^{\frac{1}{e_1}}\right) + p^{\varrho_0}\,\Psi_m^{(0)}$$

und

$$A_1'(p) = p^{\varrho_0 - \frac{m_1}{e_1}}\,\varphi_m'\left(w_1^{\frac{1}{e_1}}\right) + p^{\varrho_0 - \frac{m_1}{e_1}}\,\Psi_m'^{(0)}.$$

Wir wissen nach obigem, daß, weil p^{ϱ_0} der absolute Betrag von $A_0'(p)$ ist, der Exponent der Potenz von p, die in

$$\varphi_m\left(w_1^{\frac{1}{e_1}}\right)$$

enthalten ist,

$$\geqq \varrho_0 - \varrho_0 \quad \text{ist.}$$

Auf jeden zu $w_1^{\frac{1}{e_1}}$ gehörigen Linearfaktor entfällt demnach, weil $\frac{e \cdot f}{e_1 \cdot f_1}$ gleiche solcher Linearfaktoren vorhanden sind, ein absoluter Betrag von p, dessen Exponent

$$> \frac{\varrho_0 - \varrho_0}{\frac{e \cdot f}{e_1 \cdot f_1}}.$$

Da nun

$$\varphi_m'(x) \equiv 0 \qquad (mod\ \mathfrak{p})$$

offenbar

$$\frac{e \cdot f}{e_1 \cdot f_1} - 1$$

zu $w_1^{\frac{1}{e_1}}$ gehöriger Linearfaktoren auf der linken Seite enthält, so ist der Exponent der Potenz von p, die im 1. Posten der obigen Darstellung von $A_1'(p)$ steckt,

$$\geqq \varrho_0 - \frac{m_1}{e_1} + \frac{\varrho_0 - \varrho_0}{\frac{e \cdot f}{e_1 \cdot f_1}}\left(\frac{e \cdot f}{e_1 \cdot f_1} - 1\right)$$

also, wenn man die Klammer ausmultipliziert,

$$\geq \varrho_0 - \frac{m_1}{e_1} + \varrho_0 - \varrho_0 - \frac{\varrho_0 - \varrho_0}{\frac{e \cdot f}{e_1 \cdot f_1}}.$$

oder

$$\geqq \varrho_0 - \frac{m_1}{e_1} - \frac{\varrho_0 - \varrho_0}{\frac{e \cdot f}{e_1 \cdot f_1}}.$$

Aus der Figur ergibt sich nun, daß

$$AB = AG + GB .$$

Nun ist $$BG = EH - \frac{m_1}{e_1}$$

$$AG = CE - \frac{\varrho_0 - \varrho_0}{\frac{e \cdot f}{e_1 \cdot f_1}}$$

also durch Addition der beiden Gleichungen

$$AB = HE + EC - \frac{m_1}{e_1} - \frac{\varrho_0 - \varrho_0}{\frac{e \cdot f}{e_1 \cdot f_1}}$$

Es ist aber $HE + EC = \mu_0$,

daher $$AB = \bar{\varrho}_0 - \frac{m_1}{e_1} - \frac{\varrho_0 - \varrho_0}{\frac{e \cdot f}{e_1 \cdot f_1}}$$

Hiernach ist also der Exponent der Potenz von p, die im 1. Posten von $A_1'(p)$ steckt

$$\geqq AB ,$$

und da der Exponent des 2. Postens

$$> AB ,$$

weil ja schon

$$\bar{\varrho}_0 - \frac{m_1}{e_1} > AB,$$

so ist bewiesen, daß $\mathfrak{A}_1'$ auf oder über der Verbindungsstrecke CD liegt. Da sich in ganz derselben Weise das Gleiche für alle übrigen Punkte

$$\mathfrak{A}_k' \qquad \left(k < \frac{e\ f}{e_1\ f_1}\right)$$

zeigen läßt, so ist dargetan, daß im 2. Diagramm nur 1 Sehne höherer Steigung als im 1. Diagramm vorhanden ist, wenn man noch hinzunimmt, daß die

$$\mathfrak{A}_k' \qquad \text{für } k > \frac{e\ f}{e_1\ f_1}$$

wie aus obiger Darstellung für $A_k'(p)$ ohne weiteres hervorgeht, auf der über der einzigen Sehne des 1. Diagramms liegen.

Es hat also

$$f\left(w_1^{\frac{1}{e_1}} \cdot p^{\frac{m_1}{e_1}} + u'\right)$$

ein Diagramm, dessen Begrenzungssehne s_n größter Steigung $\frac{n}{e}$ oder in reduzierter Form $\frac{n_2}{e_2}$ allein für uns von Belang ist.

(NB. n hat nichts mehr mit dem Grad der behandelten Gleichung zu tun, dieser wird vielmehr jetzt, wie oben angegeben, durch λ bezeichnet.)

Die dieser Sehne zugeordnete Funktion φ_n hat folgende $\frac{e}{e_1} \cdot \frac{f}{f_1}$ Kongruenzwurzeln, wenn $w_1^{\frac{1}{e_1}} \cdot p^{\frac{m_1}{e_1}}$ dem Gliede $\eta_m \cdot \pi^m$ entspricht,:

1. Zeile $\left\{ \eta_n \left(\eta^{\frac{k_0}{e}} \right)^n, \quad \eta_n \left(\eta^{\frac{k_0}{e}} \cdot \omega_e^{e_1} \right)^n, \right.$

$\left. \eta_n \left(\eta^{\frac{k_0}{e}} \cdot \omega_e^{2e_1} \right)^n, \ldots \eta_n \left(\eta^{\frac{k_0}{e}} \omega_e^{\left(\frac{e}{e_1} - 1\right) e_1} \right)^n \right.$

2. Zeile $\eta_n^{p^{f_1}} \left(\eta^{\frac{k_0}{e}} \cdot p^{f_1} \right)^n \ldots \eta_n^{p^{f_1}} \left(\eta^{\frac{k_0}{e}} \cdot p^{f_1} \omega_e^{\left(\frac{e}{e_1} - 1\right) e_1} \right)^n$

3. Zeile $\eta_n^{p^{2f_1}} \left(\eta^{\frac{k_0}{e}} \cdot p^{2f_1} \right)^n, \ldots$

$\left(\frac{f}{f_1}\right)^{\text{te}}$ Zeile $\left\{ \eta_n^{p^{\left(\frac{f}{f_1} - 1\right) f_1}} \left(\eta^{\frac{k_0}{e}} \cdot p^{\left(\frac{f}{f_1} - 1\right) f_1} \right)^n, \ldots \right.$

$\left. \ldots \eta_n^{p^{\left(\frac{f}{f_1} - 1\right) f_1}} \left(\eta^{\frac{k_0}{e}} p^{\left(\frac{f}{f_1} - 1\right) f_1} \omega_e^{\left(\frac{e}{e_1} - 1\right) e_1} \right)^n, \right.$

$\frac{e}{e_1}$ Spalten

wo ω_e eine primitive $(e)^{\text{te}}$ Einheitswurzel bedeutet.

NB! Daß gerade φ_n diese Kongruenzwurzeln besitzen muß, erkennt man daraus, daß einerseits nach den gemachten Voraussetzungen

$$\eta_m \pi_1^{(0)^m} = \eta_m \pi_{e_1+1}^{(0)^m} = \eta_m \pi_{2e_1+1}^{(0)^m} = \ldots$$

und andrerseits

$$\eta_m \pi_1^{(0)^m} = \eta_m^{p^{f_1}} \pi_1^{\left(f_1\right)^m} = \eta_m^{p^{2f_1}} \pi_1^{\left(2f_1\right)^m} = \ldots \text{ ist.}$$

Wir fragen uns jetzt, welche und wieviele Kongruenzwurzeln der ersten Zeile einander gleich sind, mit anderen Worten: Für welches kleinste von Null verschiedene y ist

$$\omega_e^{ye_1n} = 1$$

oder, was dasselbe ist,

$$ye_1n \equiv 0 \pmod{e} \quad ?$$

Da $n = n_2\ (n, e)$ und $e = e_2\ (n, e)$ ist, so ergibt sich hieraus

$$y e_1 n_2 (n, e) \equiv 0 \left(mod\ e_2\ (n, e)\right) \text{ oder } y\ e_1\ n_2 \equiv 0 \pmod{e_2}.$$

Nun ist

$$(e_1\ n_2,\ e_2) = (e_1,\ e_2),$$

da

$$(n_2,\ e_2) = 1 \text{ ist.}$$

Also genügt y der Kongruenz

$$y \frac{e_1\ n_2}{(e_1,\ e_2)} \equiv 0 \left(mod \frac{e_2}{(e_1,\ e_2)}\right),$$

in der jetzt $\frac{e_1\ n_2}{(e_1,\ e_2)}$ und $\frac{e_2}{(e_1,\ e_2)}$ teilerfremd sind; also heißt das kleinste von Null verschiedene y, das der Kongruenz genügt

$$y = \frac{e_2}{(e_1,\ e_2)}.$$

Also sind nur die ersten $\frac{e_2}{(e_1,\ e_2)}$ Ausdrücke der obigen $\left(\frac{e}{e_1}\right) =$ spältigen Zeile voneinander verschieden, dann wiederholen sie sich zyklisch, und zwar gibt es im ganzen

$$\frac{\frac{e}{e_1}}{\frac{e_2}{(e_1,\ e_2)}} = \frac{e}{M\ (e_1,\ e_2)} = \left(\frac{e}{e_1}\ ,\ \frac{e}{e_2}\right)$$

Zyklen, wenn $M\ (a, b, c \cdots)$ das kleinste gemeinsame Vielfache der Größen $a,\ b,\ c,\ \cdots$ bedeutet.

Nun lassen die

$$0 \cdot e_1\ n,\ 1 \cdot e_1 n,\ 2 \cdot e_1\ n,\ \cdots \left(\frac{e_2}{(e_1,\ e_2)} - 1\right)\ e_1\ n,$$

durch e dividiert, bez. die Reste

$$0 \cdot \frac{e\,(e_1,\ e_2)}{e_2}\ ,\ 1 \cdot \frac{e\,(e_1,\ e_2)}{e_2}\ ,\ \cdots \left(\frac{e_2}{(e_1,\ e_2)} - 1\right) \frac{e\,(e_1,\ e_2)}{e_2}\ .$$

Es sind demnach die $\frac{e}{e_1}$ Ausdrücke der 1. der $\frac{f}{f_1}$ Zeilen von Seite 24 Kongruenzwurzeln von

$$\left[\left(x-\eta_n\,\eta^{\frac{k_0}{e}n}\right)\left(x-\eta_n\,\eta^{\frac{k_0}{e}n}\,\omega_e^{\frac{e(e_1,e_2)}{e_2}}\right)\left(x-\eta_n\,\eta^{\frac{k_0}{e}n}\,\omega_e^{\frac{2e(e_1,e_2)}{e_2}}\right)\cdots\right.$$

$$\left.\cdots\left(x-\eta_n\,\eta^{\frac{k_0}{e}n}\,\omega_e^{\left(\frac{e_2}{(e_1,e_2)}-1\right)\frac{e(e_1,e_2)}{e_2}}\right)\right]^{\left(\frac{e}{e_1},\frac{e}{e_2}\right)} \equiv 0 \ (mod\ \mathfrak{p}).$$

Nun sind aber die ω_e^0, $\omega_e^{\frac{e(e_1,e_2)}{e_2}}$, $\omega_e^{\frac{2e(e_1,e_2)}{e_2}}$, $\cdots$ nichts anderes als die $\frac{e_2}{(e_1,e_2)}$ verschiedenen $\left(\frac{e_2}{(e_1,e_2)}\right)$ten Einheitswurzeln, sodaß der letzte Ausdruck auch so geschrieben werden kann:

$$\left[x^{\frac{e_2}{(e_1,e_2)}}-\eta_n^{\frac{e_2}{(e_1,e_2)}}\,\eta^{\frac{k_0}{e}n\frac{e_2}{(e_1,e_2)}}\right]^{\left(\frac{e}{e_1},\frac{e}{e_2}\right)}$$

oder

$$\left[x^{\frac{e_2}{(e_1,e_2)}}-\eta_n^{\frac{e_2}{(e_1,e_2)}}\,\eta^{\frac{k_0\,n_2}{(e_1,e_2)}}\right]^{\left(\frac{e}{e_1},\frac{e}{e_2}\right)}.$$

Ganz entsprechend sind dann die $\frac{e}{e_1}$ Ausdrücke der 2. der $\frac{f}{f_1}$ Zeilen auf S. 24 Wurzeln von

$$\left[x^{\frac{e_2}{(e_1,e_2)}}-\left(\eta_n^{\frac{e_2}{(e_1,e_2)}}\,\eta^{\frac{k_0\,n_2}{(e_1,e_2)}}\right)^{p^{f_1}}\right]^{\left(\frac{e}{e_1},\frac{e}{e_2}\right)} \equiv 0 \ (mod\ \mathfrak{p}),$$

u. s. f.; die Ausdrücke der letzten dortigen Zeile sind schließlich Wurzeln von

$$\left[x^{\frac{e_2}{(e_1,e_2)}}-\left(\eta_n^{\frac{e_2}{(e_1,e_2)}}\,\eta^{\frac{k_0\,n_2}{(e_1,e_2)}}\right)^{p^{\left(\frac{f}{f_1}-1\right)f_1}}\right]^{\left(\frac{e}{e_1},\frac{e}{e_2}\right)} \equiv 0 \ (mod\ \mathfrak{p}).$$

Die Größe $\eta_n^{e_2}\,.\,\eta^{k_0\,n_2}$ ist sicher eine $(p^f-1)^{\text{te}}$ Einheitswurzel, für die wir bisweilen kurz η_τ schreiben wollen. Gesetzt, η_τ passe zum Exponenten f_2, einem Teiler von f, so fragen wir jetzt: Für welches kleinste von Null verschiedene y ist

$$\eta_\tau^{p^{yf_1}} = \eta_\tau \quad ?$$

Diese Frage reduziert sich aber auf die Frage nach der kleinsten von Null verschiedenen Lösung der Kongruenz

$$yf_1 \equiv 0 \pmod{f_2}$$

oder

$$y \frac{f_1}{(f_1, f_2)} \equiv 0 \left(\bmod \frac{f_2}{(f_1, f_2)} \right).$$

Man findet sofort

$$y = \frac{f_2}{(f_1, f_2)}.$$

Also sind nur die $\frac{f_2}{(f_1, f_2)}$ ersten der obigen eckigen Klammern voneinander verschieden, dann herrscht zyklische Wiederholung, und zwar gibt es im ganzen

$$\frac{f}{\frac{f_1}{f_2}} = \frac{f}{M(f_1, f_2)} = \left(\frac{f}{f_1}, \frac{f}{f_2} \right)$$
$$(f_1, f_2)$$

solcher Zyklen. Somit folgt, daß die $\frac{e}{e_1} \cdot \frac{f}{f_1}$ Größen von S. 24 Kongruenzwurzeln sind von

$$\varphi_n \equiv \left[\left\{ x^{\frac{e_2}{(e_1, e_2)}} - \left(\eta_n^{\frac{e_2}{(e_1, e_2)}} \cdot \eta^{\frac{k_0 n_2}{(e_1, e_2)}} \right) \right\} \times \right.$$

$$\left\{ x^{\frac{e_2}{(e_1, e_2)}} - \left(\eta_n^{\frac{e_2}{(e_1, e_2)}} \cdot \eta^{\frac{k_0 n_2}{(e_1, e_2)}} \right)^{p^{f_1}} \right\} \times$$

$$\left\{ x^{\frac{e_2}{(e_1, e_2)}} - \left(\eta_n^{\frac{e_2}{(e_1, e_2)}} \cdot \eta^{\frac{k_0 n_2}{(e_1, e_2)}} \right)^{p^{2f_1}} \right\} \times - - - - - - - \times$$

$$\left. \left\{ x^{\frac{e_2}{(e_1, e_2)}} - \left(\eta_n^{\frac{e_2}{(e_1, e_2)}} \cdot \eta^{\frac{k_0 n_2}{(e_1, e_2)}} \right)^{p^{\left(\frac{f_2}{(f_1, f_2)} - 1\right) f_1}} \right\} \right] \left(\frac{e}{e_1}, \frac{e}{e_2} \right) \left(\frac{f}{f_1}, \frac{f}{f_2} \right)$$
$$\equiv 0 \pmod{\mathfrak{p}}.$$

Setzt man dieses Verfahren weiter fort, so findet man, daß der Begrenzungssehne höchster Steigung $\frac{o}{e} = \frac{o_3}{e_3}$ (wo $(o_3, e_3) = 1$) des Diagramms von

$$f\left(r_m \pi_1^{(0)^m} + r_n \pi_1^{(0)^n} + u''\right) = 0$$

eine Koeffizientenkongruenz

$$\varphi_o \equiv 0 \pmod{\mathfrak{p}}$$

zugeordnet ist vom Grade

$$\left(\frac{e}{e_1}, \frac{e}{e_2}\right)\left(\frac{f}{f_1}, \frac{f}{f_2}\right).$$

Und zwar ist

$$\varphi_o \equiv \left[\left\{ x^{\frac{e_3}{\left(\frac{e_1 e_2}{(e_1, e_2)}, e_3\right)}} - \left(\eta_o^{\frac{e_3}{\left(\frac{e_1 e_2}{(e_1, e_2)}, e_3\right)}} \eta^{\frac{k_0 o_3}{\left(\frac{e_1 e_2}{(e_1, e_2)}, e_3\right)}} \right) \right\} \times \right.$$

$$\left\{ x^{\frac{e_3}{\left(\frac{e_1 e_2}{(e_1, e_2)}, e_3\right)}} - \left(\eta_o^{\frac{e_3}{\left(\frac{e_1 e_2}{(e_1, e_2)}, e_3\right)}} \eta^{\frac{k_0 o_3}{\left(\frac{e_1 e_2}{(e_1, e_2)}, e_3\right)}} \right) p^{\frac{f_1 f_2}{(f_1, f_2)}} \right\} \times$$

$$\left\{ x^{\frac{e_3}{\left(\frac{e_1 e_2}{(e_1, e_2)}, e_3\right)}} - \left(\eta_o^{\frac{e_3}{\left(\frac{e_1 e_2}{(e_1, e_2)}, e_3\right)}} \eta^{\frac{k_0 o_3}{\left(\frac{e_1 e_2}{(e_1, e_2)}, e_3\right)}} \right) p^{\frac{2 f_1 f_2}{(f_1, f_2)}} \right\} \times$$

$$\left\{ . \; . \; . \; . \; . \; . \; . \; . \; . \right\} \times \; . \; . \; . \; . \; . \; . \; . \; . \times$$

$$\left. \left\{ x^{\frac{e_3}{\left(\frac{e_1 e_2}{(e_1, e_2)}, e_3\right)}} - \left(\eta_o^{\frac{e_3}{\left(\frac{e_1 e_2}{(e_1, e_2)}, e_3\right)}} \eta^{\frac{k_0 o_3}{\left(\frac{e_1 e_2}{(e_1, e_2)}, e_3\right)}} \right) p^{\left(\frac{f_3}{\left(\frac{f_1 f_2}{(f_1, f_2)}, f_3\right)} - 1\right) \frac{f_1 f_2}{(f_1, f_2)}} \right\} \right]^{\left(\frac{e}{e_1}, \frac{e}{e_2}, \frac{e}{e_3}\right)\left(\frac{f}{f_1}, \frac{f}{f_2}, \frac{f}{f_3}\right)}$$

wenn man annimmt, daß die $(p^f-1)^{\text{te}}$ Einheitswurzel

$$\eta_0^{e_3} \cdot \eta^{k_0 o_3}$$

zum Exponenten f_3 paßt.

Allgemein gehört zu einer Sehne höchster Steigung

$$\frac{\overline{i}}{e} = \frac{\overline{i_i}}{e_i}, \quad \left[\left(\overline{i_i}, e_i\right) = 1\right],$$

späterer Diagramme die Koeffizientenkongruenz

$$\varphi_{\overline{i}}$$

$$\varphi_{\overline{i}}(x) \equiv \left[\left\{ x^{\frac{e_i}{(M(e_1, e_2, \ldots e_{i-1}), e_i)}} - \left(\eta_{\overline{i}}^{\frac{e_i}{(M(e_1, e_2, \ldots e_{i-1}), e_i)}} \eta^{\frac{k_0 \overline{i_i}}{(M(e_1, e_2, \ldots e_{i-1}), e_i)}} \right) \right\} \times \right.$$

$$\left\{ x^{\frac{e_i}{(M(e_1, e_2, \ldots e_{i-1}), e_i)}} - \left(\eta_{\overline{i}}^{\frac{e_i}{(M(e_1, e_2, \ldots e_{i-1}), e_i)}} \eta^{\frac{k_0 \overline{i_i}}{(M(e_1, e_2, \ldots e_{i-1}), e_i)}} \right)^{p^{M(f_1, f_2, \ldots f_{i-1})}} \right\} \times$$

$$\left\{ x^{\frac{e_i}{(M(e_1, e_2, \ldots e_{i-1}), e_i)}} - \left(\eta_{\overline{i}}^{\frac{e_i}{(M(e_1, e_2, \ldots e_{i-1}), e_i)}} \eta^{\frac{k_0 \overline{i_i}}{(M(e_1, e_2, \ldots e_{i-1}), e_i)}} \right)^{p^{2M(f_1, f_2, \ldots f_{i-1})}} \right\} \times$$

$$\left\{ \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \right\} \times \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \cdot \times$$

$$\left. \left\{ x^{\frac{e_i}{(M(e_1, e_2, \ldots e_{i-1}), e_i)}} - \left(\eta_{\overline{i}}^{\frac{e_i}{(M(e_1, e_2, \ldots e_{i-1}), e_i)}} \eta^{\frac{k_0 \overline{i_i}}{(M(e_1, e_2, \ldots e_{i-1}), e_i)}} \right)^{p^{\left(\frac{f_i}{(M(f_1, f_2, \ldots f_{i-1}), f_i)} - 1\right) M(f_1, f_2, \ldots f_{i-1})}} \right\} \right]^{\left(\frac{e}{e_1}, \frac{e}{e_2}, \ldots \frac{e}{e_i}\right)\left(\frac{f}{f_1}, \frac{f}{f_2}, \ldots \frac{f}{f_i}\right)} \equiv 0 \pmod{\mathfrak{p}},$$

wobei vorausgesetzt wird, daß die $(p^f-1)^{\text{te}}$ Einheitswurzel

$$\eta_i^{e_i} \cdot \eta^{k_0 i_i}$$

zum Exponenten f_i paßt.

Da $f(u)$ als irreduzibel angenommen wurde, so wird schließlich in vollständiger Analogie zu H & L S. 57 der Exponent der eckigen Klammer eines bestimmten φ gleich 1, d. h. nichts anderes als, die zuvor ermittelten Glieder der Wurzelreihe machen ihren irregulären Teil aus. Die Einheit aber, mit der der absolute Betrag

$$p^{\frac{r}{r}}_{\frac{e}{r}}$$

des 1. regulären Gliedes zu multiplizieren ist, ergibt sich aus der Kongruenz

$$\varphi_r(x) \equiv x - \eta_r \cdot \eta^{\frac{k_0 r}{r}}_{\frac{e}{r}} \equiv 0 \pmod{\mathfrak{p}} .$$

Denn nehmen wir an,

$$\varphi_i(x) \equiv 0 \pmod{\mathfrak{p}}$$

sei insbesondere gerade die letzte Kongruenz des irregulären Teils, so läßt sich die eben erwähnte Kongruenz

$$\varphi_r(x) \equiv x - \eta_r \cdot \eta^{\frac{k_0 r}{r}}_{\frac{e}{r}} \equiv 0 \pmod{\mathfrak{p}}$$

sofort aus $\varphi_i(x)$ ableiten, wenn man darin von i zu $i+1$ übergeht und bedenkt, daß dann

$$M(e_1, e_2, \cdots e_i) = e ,$$
$$M(f_1, f_2, \cdots f_i) = f$$

und $e_{i+1} = e_r$ ein Teiler von e und f_{i+1} ein Teiler von f ist.

Es ist jetzt e bekannt als kleinstes gemeinsames Vielfaches von $e_1, e_2, \cdots e_i$, wo e_1 bis e_i die reduzierten Nenner der den irregulären Gliedern zugeordneten Steigungen der betreffenden Sehnen sind. $\lambda = e \cdot f$ ist der Grad der 1. Kongruenz

$$\varphi_m(x) \equiv 0 \pmod{\mathfrak{p}} ,$$

f ist dann ebenfalls bekannt.

Aus der 1. Kongruenz $\varphi_m(x) \equiv 0 \pmod{\mathfrak{p}}$ ermittelt man, wie oben angegeben, als Wurzel eine Größe, die eine $(e_1)^{\text{te}}$ Wurzel aus einer $(p^f - 1)^{\text{ten}}$ Einheitswurzel ist, die der Annahme nach zum Exponenten f_1 paßt:

$$\sqrt[e_1]{\eta_\sigma} = \sqrt[e_1]{\eta_m}^{e_1} \cdot \eta^{k_0 m_1} .$$

Die Einheit, die im 2. Gliede von u_0 vorkommt, ermittelt man aus $\varphi_n^{(x)} \equiv 0 \ (mod\ \mathfrak{p})$ als $(e_2)^{\text{te}}$ Wurzel aus einer $(p^f - 1)^{\text{ten}}$ Einheitswurzel, die zum Exponenten f_2 paßt usw.

Die Einheit, die in dem letzten irregulären Gliede $\varepsilon_i p^{t_i}$ von u_0 vorkommt, ergibt sich aus $\varphi_i^{(x)} \equiv 0 \ (mod\ \mathfrak{p})$ als $(e_i)^{\text{te}}$ Wurzel aus einer $(p^f - 1)^{\text{ten}}$ Einheitswurzel, die zum Exponenten f_i paßt.

Alle diese Kongruenzwurzeln können durch eine endliche Anzahl von Versuchen gefunden werden. Aus dem Grad $\lambda = e \cdot f$ der 1. Kongruenz $\varphi_m(x) \equiv 0 \pmod{\mathfrak{p}}$, dem Exponenten der eckigen Klammer von $\varphi_m(x)$:

$$\frac{e \cdot f}{e_1 \cdot f_1} = l$$

und e_1, dem reduzierten Nenner der Steigung der Sehne des 1. Diagramms, ergibt sich

$$f_1 = \frac{\lambda}{e_1 \, l},$$

und man hat somit nur die in endlicher Anzahl vorhandenen $(p^{f_1} - 1)^{\text{ten}}$ Einheitswurzeln der Reihe nach vorzunehmen, eine beliebige $(e_1)^{\text{te}}$ Wurzel aus einer von ihnen zu ziehen und zu probieren, ob diese Größe

$$\varphi_m^{(x)} \equiv 0 \ (mod\ \mathfrak{p})$$

befriedigt.

Bei Behandlung von

$$\varphi_n^{(x)} \equiv 0 \ (mod\ \mathfrak{p})$$

kennt man

$$e_1, \ e_2 \text{ und } \lambda,$$

f_2 ist also sicher ein Teiler von

$$\frac{\lambda}{M\,(e_1,\ e_2)}.$$

Man hat also jetzt unter den $(p^{\frac{\lambda}{M(e_1, e_2)}} - 1)^{\text{ten}}$ Einheitswurzeln, unter denen sicher die hier in Betracht kommende $(p^{f_2} - 1)^{\text{te}}$ Einheitswurzel steckt, eine zu wählen, die $(e_2)^{\text{te}}$ Wurzel aus ihr zu ziehen und zu ermitteln, ob diese Wurzel

$$\varphi_n^{(x)} \equiv 0 \ \ (mod\ \mathfrak{p})$$

erfüllt, u. s. f.

Bei Lösung der Kongruenz

$$\varphi_{\overline{i}}^{\lambda}(x) \equiv 0 \pmod{\mathfrak{p}}$$

bieten die $(p^{\overline{M}(e_1, e_2, \ldots, e_i)} - 1)^{\text{ten}}$ Einheitswurzeln den Ausgangspunkt.

Man bemerkt, daß von der 3. Kongruenz an die Anzahl der Größen, unter denen man zu wählen hat, allenfalls die gleiche ist wie bei der vorhergehenden Kongruenz oder aber abnimmt.

Wir erwähnten schon auf Seite 33 kurz, daß man, weil $f(u)$ als im Bereich der rationalen p=adischen Zahlen irreduktibel vorausgesetzt ist, unter fast wörtlicher Anlehnung an H & L. S. 56 bis 59 und S. 65 bis 67 zeigen kann, daß man schließlich zu einem Diagramm kommt, dessen Sehne maximaler Steigung eine Kongruenz 1. Grads

$$\varphi_r^{(x)} \equiv 0 \pmod{\mathfrak{p}}$$

zugeordnet ist, die dann die Einheit ε_r des sog. 1. regulären Glieds der Wurzelreihe u_0 liefert. Insbesondere ergibt sich aus H & L. S. 67 durch Analogie, daß man die sämtlichen regulären Glieder von u_0 durch ein rekurrierendes Verfahren bestimmen kann.

Ist nämlich $\varepsilon_{r+1} p^{t_{r+1}}$ ein reguläres Glied der Wurzel u_0 der Gleichung $f(u, p) = 0$ für den Bereich von p und $u^{(r)}$ das Aggregat aller vorangehenden Glieder der Reihe u_0, so ist $\varepsilon_{r-1} p^{t_{r-1}}$ gleich dem Anfangsglied der Entwickelung von

$$-\frac{f(u^{(r)})}{f'(u^{(r)})}$$

nach Potenzen von p.

Wir kommen nach Ermittelung der Primzahl π und der Koeffizienten des irregulären Teils von u_0 auf die Anwendung des Verfahrens zurück. Jetzt ziehen wir aus ihm nur den Schluß daß die Bestimmung von π nur von den irregulären Gliedern von u_0 abhängt.

Wir wenden uns daher jetzt zur Bestimmung einer Eisensteinschen Gleichung für die Primzahl π unserer Reihe u_0.

Wir hatten bei der Lösung der Kongruenzen

$$\varphi(x) \equiv 0 \pmod{\mathfrak{p}}$$

bestimmte $(p^f - 1)^{\text{te}}$ Einheitswurzeln heranzuziehen, und zwar

bei $\varphi_m(x) \equiv 0 \pmod{\mathfrak{p}}$ die Einheitswurzel $\eta_\sigma = \eta_m^{e_1} \cdot \eta^{k_0 \cdot m_1}$

bei $\varphi_n(x) \equiv 0 \pmod{\mathfrak{p}}$ die Einheitswurzel $\eta_\tau = \eta_n^{e_2} \cdot \eta^{k_0 \cdot n_2}$

bei $\varphi_o(x) \equiv 0 \pmod{\mathfrak{p}}$ die Einheitswurzel $\eta_o^{e_3} \cdot \eta^{k_0 \cdot o_3}$

. . . . . .

bei $\varphi_{\bar{i}}(x) \equiv 0 \pmod{\mathfrak{p}}$ die Einheitswurzel $\eta_{\bar{i}}^{e_i} \cdot \eta^{k_0 \cdot i_i}$.

Wir stellen alle diese Einheitswurzeln als Potenzen derjenigen primitiven $(p^f - 1)^{\text{ten}}$ Einheitswurzel η dar, die wir der gesuchten Eisensteinschen Gleichung

$$\pi^e = \eta^{k_0} \cdot p$$

zu Grunde legen wollen. Dann ist nach den Darlegungen in H S. 202/203 nach Festlegung des η der Exponent k_0 eindeutig bestimmbar.

Es sei

$$\eta_m = \eta^{\bar{m}}, \quad \eta_n = \eta^{\bar{n}}, \quad \eta_o = \eta^{\bar{o}}, \quad \ldots \ldots \eta_{\bar{i}} = \eta^{\bar{\bar{i}}}.$$

Dann ist

$$\eta_m^{e_1} \cdot \eta^{k_0 m_1} = \eta^{\bar{m} e_1 + k_0 m_1} = \eta^{d_1},$$

wenn $\bar{m} e_1 + k_0 m_1 \equiv d_1 \pmod{p^f - 1}$ ist.

Ferner:

$$\eta_n^{e_2} \cdot \eta^{k_0 n_2} = \eta^{\bar{n} e_2 + k_0 n_2} = \eta^{d_2},$$

wenn $\bar{n} e_2 + k_0 n_2 \equiv d_2 \pmod{p^f - 1}$.

Ebenso

$$\eta_o^{e_3} \cdot \eta^{k_0 o_3} = \eta^{\bar{o} e_3 + k_0 o_3} = \eta^{d_3},$$

wo $o e_3 + k_0 o_3 \equiv d_3 \pmod{p^f - 1}$

usw.

Endlich

$$\eta_{\overline{i}}^{e_i} \cdot \eta^{k_0 \overline{i}_i} = \eta^{\overline{\overline{i}\, e_i + k_0 \overline{i}_i}} = \eta^{d_i},$$

wo $\overline{\overline{i}\, e_i + k_0 \overline{i}_i} \equiv d_i \pmod{p^f - 1}$ ist.

Wir haben uns jezt die Kongruenzen

$$\begin{aligned}
\overline{m}\, e_1 + k_0 m_1 &\equiv d_1 \pmod{p^f - 1} \\
\overline{n}\, e_2 + k_0 n_2 &\equiv d_2 \pmod{p^f - 1} \\
\overline{o}\, e_3 + k_0 o_3 &\equiv d_3 \pmod{p^f - 1} \\
&\cdots\cdots\cdots\cdots \\
\overline{\overline{i}\, e_i} + k_0 \overline{i}_i &\equiv d_i \pmod{p^f - 1}
\end{aligned}$$

zu betrachten. Wir kennen darin die e_i, d_i und m_1, n_2, o_3, $\cdots\cdots i_i$.

Fassen wir in der ersten dieser Kongruenzen k_0 für einen Augenblick als bereits bekannt auf, so könnte die Kongruenz

$$x\, e_1 + k_0 m_1 \equiv d_1 \pmod{p^f - 1}$$

dann und nur dann gelöst werden, wenn

$$d_1 - k_0 m_1 \equiv 0 \pmod{(e_1, p^f - 1)}$$

ist, oder wenn

$$k_0 m_1 \equiv d_1 \pmod{(e_1, p^f - 1)}.$$

Nun ist bekanntlich $(m_1, e_1) = 1$,

also auch $(m_1, (e_1, p^f - 1)) = 1$.

Also hat die letzte Kongruenz dann eine Lösung nach k_0, die *modulo* $(e_1, p^f - 1)$ eindeutig bestimmt ist:

$$k_0 \equiv \tfrac{d_1}{m_1} \left(\mathit{mod}\ (e_1, p^f - 1)\right) .$$

Hierin kennen wir

1) d_1 als Exponenten von η^{d_1}, welches diejenige $(p^f - 1)^{\text{te}}$ Einheitswurzel ist, die bei der Lösung der Kongruenz

$$\varphi_m(x) \equiv 0 \pmod{\mathfrak{p}}$$

herangezogen wurde.

2) m_1 als reduzierten Zähler der Steigung der einzigen Sehne des 1. Diagramms;

3) e_1 als reduzierten Nenner des gleichen Bruches;

4) p^f-1, da p gegeben und f nach Abschluß des irregulären Teils der Reihe u_0 als $\frac{\lambda}{e}$, wo $e = M(e_1, e_2, \cdots e_i)$ und λ der Grad der gegebenen Gleichung, bekannt ist.

Nur wenn wir k_0 also aus der Kongruenz

$$k_0 \equiv \frac{d_1}{m_1} \ (mod\ (e_1, p^f-1))$$

bestimmen, — und dies ist eindeutig möglich — kann die Kongruenz

$$\overline{m}\, e_1 + k_0 m_1 \equiv d_1 \ (mod\ p^f-1)$$

nach $\overline{m}$ gelöst werden.

Was die 2. der Kongruenzen von Seite 37 anlangt, so ist für ihre Lösung nach n Bedingung, daß

$$d_2 - k_0 n_2 \equiv 0 \ (mod\ (e_2, p^f-1))$$

oder $k_0 n_2 \equiv d_2 \ (mod\ (e_2, p^f-1))$ ist. Da

$$(e_2, n_2) = 1,$$

also auch $(n_2, (e_2, p^f-1)) = 1$ ist,

ergibt sich hieraus wieder für k_0 die eindeutig erfüllbare Forderung

$$k_0 \equiv \frac{d_2}{n_2} \ (mod\ (e_2, p^f-1)).$$

Man sieht sofort, daß man aus den i Kongruenzen auf Seite 37, wenn man in gleicher Weise weitergeht, für k_0 die i Kongruenzen erhält:

$$k_0 \equiv \frac{d_1}{m_1} \ (mod\ (e_1, p^f-1))$$

$$k_0 \equiv \frac{d_2}{n_2} \ (mod\ (e_2, p^f-1))$$

$$k_0 \equiv \frac{d_3}{o_3} \ (mod\ (e_3, p^f-1))$$

— — — — — — — — — —

$$k_0 \equiv \frac{d_i}{i_i} \ (mod\ (e_i, p^f-1)).$$

Daß diese Kongruenzen miteinander verträglich sein müssen, d. h., daß die endliche Anzahl von Bedingungen

$$k_\mu \equiv k_\nu \pmod{(e_\mu, e_\nu, p^f-1)}$$

erfüllt ist, wo k_μ die Lösung der μ^{ten} und k_ν die Lösung der ν^{ten} Kongruenz sein soll, ergibt sich daraus, daß widrigenfalls k_0 aus diesen Kongruenzen nicht als *mod* (e, p^f-1) eindeutig bestimmte Zahl ermittelt werden könnte, was mit dem Satze in H S. 202/203 in Widerspruch steht.

Dann bestimmt sich aber in der Tat nach bekanntem Verfahren der Zahlentheorie aus jenen i Kongruenzen eine Zahl

$$k_0 \quad mod\left(M\left((e_1, p^f-1), (e_2, p^f-1), \cdots, (e_i, p^f-1)\right)\right)$$

eindeutig, die alle jene i Forderungen erfüllt.

Nun ist

$$M\left((e_1, p^f-1), (e_2, p^f-1), \cdots, (e_i, p^f-1)\right) = (e, p^f-1),$$

da ja

$$M(e_1, e_2, \cdots, e_i) = e \quad \text{ist.}$$

k_0 ist also dann *modulo* (e, p^f-1) eindeutig berechnet.

Als Eisensteinsche Gleichung für die Primzahl π unserer Wurzelreihe u_0 ergibt sich dann

$$\pi^e = \eta^{k_0} \cdot p,$$

wo η dieselbe $(p^f-1)^{\text{te}}$ primitive Einheitswurzel ist, die zur Darstellung der $(p^f-1)^{\text{ten}}$ Einheitswurzeln η_σ, η_τ u. s. w. benutzt wurde (S. 36).

Eine Wurzel der letzten Gleichung wählen wir nun als Entwickelungszahl π unserer Reihe u_0.

Dividiert man jetzt das bisher in der Form

$$w_1^{\frac{1}{e_1}} \cdot p^{\frac{m_1}{e_1}}$$

dargestellte 1. Glied unserer Reihe u_0 durch π^m, so ist nach der getroffenen Wahl von k_0 der Quotient

$$\frac{w_1^{\frac{1}{e_1}} \cdot p^{\frac{m_1}{e_1}}}{\pi^m}$$

nichts anderes als der gesuchte Entwickelungskoeffizient

$$\eta_m$$

unseres 1. Glieds, nämlich eine $(p^f-1)^{\text{te}}$ Einheitswurzel.

In gleicher Weise erhält man bei allen übrigen irregulären Gliedern von u_0 die Koeffizienten als $(p^f - 1)^{\text{te}}$ Einheitswurzeln, wenn man der Reihe nach die Quotienten

$$\frac{w_2^{\frac{1}{e_2}} \cdot p^{\frac{n_2}{e_2}}}{\pi^n}, \quad \frac{w_3^{\frac{1}{e_3}} \cdot p^{\frac{o_3}{e_3}}}{\pi^o} \quad \cdots \cdots$$

$$\frac{w_i^{\frac{1}{e_i}} \cdot p^{\frac{\bar{\imath}_i}{e_i}}}{\pi^{\bar{\imath}}}$$

bildet; dies sind dann beziehlich die Entwickelungskoeffizienten

$$\eta_n, \ \eta_o, \ \cdots \ \eta_{\bar{\imath}}$$

Damit ist der irreguläre Teil von u_o in der verlangten Art dargestellt. Die Glieder des regulären Teils von u_0 ergeben sich jetzt nach der schon auf S. 35 erwähnten Art direkt in der gewünschten Form, d. h. mit der Entwickelungszahl π und $(p^f - 1)^{\text{ten}}$ Einheitswurzeln als Koeffizienten, wenn man das Aggregat $u^{(r)}$ aller vorangehenden Glieder der Reihe u_0 in der eben besprochenen Weise nach Potenzen von π entwickelt und dann von dem Ausdruck

$$-\frac{f(u^{(r)})}{f'(u^{(r)})}$$

das Anfangsglied darstellt; dieses ist alsdann das auf $u^{(r)}$ folgende reguläre Glied von u_0. In dieser Weise fortfahrend können jetzt beliebig viele Glieder von u_0 auf einfache Art berechnet werden. (Vgl. H & L S. 67 unten.)

Lebenslauf.

Philipp Voll, geboren am 13. Juli 1885 zu Frankfurt a. M., preußischer Staatsangehörigkeit, katholischer Religion, besuchte von Ostern 1892 bis Ostern 1904 in seiner Vaterstadt die Klinger-Oberrealschule, die ihm das Reifezeugnis erteilte. Hierauf studierte er Mathematik, Physik und Geographie und zwar von Ostern 1904 bis Ostern 1905 auf der Universität München, im Sommersemester 1905 auf der Universität Berlin, im Wintersemester 1905/06 in Heidelberg, endlich von Ostern 1906 bis Herbst 1908 in Marburg. Im Frühjahr 1909 legte er in Marburg die Prüfung für die Lehrbefähigung an höheren Schulen ab. Er leistete das Seminarjahr an der Klingerschule, das Probejahr an der Adlerflychtschule zu Frankfurt a. M. ab und wurde hier am 1. April 1911 als Oberlehrer für die städtischen höheren Lehranstalten angestellt. Das Rigorosum bestand er am 3. März 1915. Er hielt sich seit dem Rigorosum bis zur Promotion in Frankfurt a. M. auf.

Es sei mir auch an dieser Stelle gestattet, Herrn Geh. Reg.-Rat Prof. Dr. Hensel nochmals meinen herzlichsten Dank auszusprechen für die Anregung zu dieser Arbeit und für die große Unterstützung, die mir von seiner Seite in gütigster Weise zu Teil wurde.